

19. p -groups

Definition 19.1. A group of order p^n , where p is a prime, is called a p -group.

Clearly \mathbb{Z}_p is the only p -group of order p . In this section we shall classify all p -groups of order p^2 , and we will also show that every p -group is nilpotent. To do this we need the following two lemmas.

Lemma 19.2. *If G is a group of order p^n , where p is a prime, then G has a non-trivial centre.*

Proof. Consider the Class Equation for G :

$$|G| = |Z(G)| + \sum_{i=1}^r [G : N(x_i)].$$

All the summands $[G : N(x_i)]$ are divisible by p , and since $|G|$ is divisible by p we conclude that $|Z(G)|$ must be divisible by p as well. Therefore, $Z(G)$ must be non-trivial. ■

Lemma 19.3. *Let G be a group. If $G/Z(G)$ is a cyclic group, then G is abelian and $G = Z(G)$.*

Proof. Write Z for $Z(G)$, and let aZ be a generator for G/Z . Then the cosets of Z are $a^i Z$ ($i \in \mathbb{Z}$). Let $x, y \in G$; then we must have $xZ = a^i Z$ and $yZ = a^j Z$ for some $i, j \in \mathbb{Z}$.

Since $x \in xZ$ and $y \in yZ$, we have $x = a^i z_1$, $y = a^j z_2$, where $z_1, z_2 \in Z$. Then we have

$$xy = a^i z_1 a^j z_2 = a^{i+j} z_1 z_2 = a^j z_2 a^i z_1 = yx,$$

and hence G is abelian. ■

Theorem 19.4. *Every group of order p^2 where p is a prime is either isomorphic to \mathbb{Z}_{p^2} or to $\mathbb{Z}_p \oplus \mathbb{Z}_p$.*

Proof. Let G be a group of order p^2 . By Lemma 19.2, $Z(G)$ is non-trivial, and hence it has order p or p^2 . If $|Z(G)| = p$ then $G/Z(G)$ would have order p , and would be cyclic by Theorem 6.10. But then, by Lemma 19.3, we would have that G is abelian and $G = Z(G)$, which is a contradiction. Therefore, we conclude that $Z(G)$ has order p^2 , and is equal to G . We conclude that G is abelian. The theorem now follows from the Fundamental Theorem for Finite Abelian Groups. ■

Remark 19.5. It is not true that every p -group is abelian. Indeed, Q_8 and D_4 are non-abelian 2-groups. More generally, let p be a prime, and on the set $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ define a multiplication by

$$(a, b, c)(d, e, f) = (a + d, b + e, c + f - bd).$$

The resulting structure is a non-abelian group of order p^3 .

Theorem 19.6. *Every p -group G is nilpotent.*

Proof. (Omitted in lectures)

Define $Z_0 = \{e\}$ and $Z_1 = Z(G)$. Note that $Z_1 \neq \{e\}$ by Lemma 19.2. The quotient G/Z_1 is again p -group, and hence has a non-trivial centre. By The Correspondence Theorem we can write $Z(G/Z_1) = Z_2/Z_1$. By continuing this process we obtain a series $\{e\} = Z_0 \leq Z_1 \leq Z_2 \leq \dots \leq Z_m = G$ such that $Z_{i+1}/Z_i = Z(G/Z_i)$. This last condition means that for every $x \in Z_{i+1}$ and every $y \in G$ the cosets xZ_i and yZ_i commute. Therefore we have $[x, y] \in Z_i$, and hence

$$[Z_{i+1}, G] \leq Z_i. \tag{4.5}$$

We now prove that for every $i = 1, \dots, m$ we have

$$\gamma_i(G) \leq Z_{m-i} \tag{4.6}$$

by induction on i . For $i = 0$ we have $\gamma_0(G) = G = Z_m$. If (4.6) is correct for some i then for $i + 1$ we have

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [Z_{m-i}, G] \leq Z_{m-i-1},$$

where (4.5) has been used in the last step.

If we put $i = m$ in (4.6), we obtain $\gamma_m(G) \leq Z_0 = \{e\}$. Therefore G is nilpotent, as required. ■

20. Sylow Theorems

Lagrange's theorem asserts that the order of a subgroup divides the order of the group. One may ask the converse question: given a finite group G and a number m dividing $|G|$, does G contain a subgroup of order m ? The following example shows that the answer is negative in general:

Example 20.1. The alternating group A_5 has order 60. Assume that it has a subgroup H of order 30. Since $[A_5 : H] = 2$ it follows that H is normal in A_5 , which contradicts the fact that A_5 is simple (Theorem 13.3).

The first Sylow theorem gives a special case where the answer to the above question is positive.

Theorem 20.2 (The first Sylow theorem) *Let G be a finite group, and let $|G| = p^n m$, where p is a prime and $\gcd(p, m) = 1$. Then for each i , $1 \leq i \leq n$, G contains a subgroup of order p^i .*

Proof. We prove the theorem by induction on the order of G . If $|G| = 1$ there is nothing to prove, so let us assume that $|G| > 1$.

Let, as in Theorem 18.6, C_1, \dots, C_r be the conjugacy classes of G containing more than one element, and let $x_j \in C_j$, $1 \leq j \leq r$, be representatives of these classes. By Theorem 18.4 we have

$$1 < |C_j| = [G : N(x_j)],$$

and therefore $N(x_j)$ is a proper subgroup of G . If p^n divides the order of $N(x_j)$ for some j , then, by induction, $N(x_j)$ contains a subgroup of order p^i for each i , $1 \leq i \leq n$. But $N(x_j) \leq G$, and hence G contains a subgroup of order p^i for each i , $1 \leq i \leq n$.

Let us now assume that p^n does not divide $|N(x_j)|$ for any j , $1 \leq j \leq r$. By Lagrange's Theorem we have

$$|G| = |N(x_j)||[G : N(x_j)],$$

and since $p^n \nmid |G|$, we conclude that p divides $[G : N(x_j)]$ for all j , $1 \leq j \leq r$.

From the class equation of G :

$$|G| = |Z(G)| + \sum_{j=1}^r [G : N(x_j)]$$

we now conclude that p divides $|Z(G)|$.

$Z(G)$ is an abelian group, and by the Fundamental Theorem for Finite Abelian Groups, it is isomorphic to a direct sum of cyclic groups of prime power orders. At least one of these summands must be \mathbb{Z}_{p^l} for some l . But then $p^{l-1}\mathbb{Z}_{p^l}$ is a subgroup of \mathbb{Z}_{p^l} isomorphic to \mathbb{Z}_p . We conclude that $Z(G)$ contains a subgroup N of order p .

Since elements of $Z(G)$ commute with all elements of G , it follows that $N \trianglelefteq G$. Form the quotient group G/N ; it has order $p^{n-1}m < |G|$. By induction G/N contains a subgroup of order p^j for every j , $1 \leq j \leq n-1$. By the Correspondence Theorem, every such subgroup of G/N has a form K/N , where K is a subgroup of G containing N . But then $|K| = |K/N||N| = p^j p = p^{j+1}$. Therefore G contains subgroups of orders p^2, \dots, p^n . G also contains a subgroup of order p , namely N itself, and this completes the proof of the theorem. ■

Definition 20.3. If G is a finite group of order $p^n m$, where p is a prime and $\gcd(p, m) = 1$, then every subgroup of order p^n is called a *Sylow p -subgroup* of G .

The first Sylow theorem states that a finite group G contains a Sylow p -subgroup for every prime p dividing $|G|$. The Second Sylow Theorem asserts that all Sylow p -subgroups are related via conjugation.

Theorem 20.4 (The second Sylow theorem) *Let G be a finite group and let p be a prime dividing the order of G . Every conjugate of a Sylow p -subgroup of G is again a Sylow p -subgroup of G . Conversely, every two Sylow p -subgroups are conjugate in G .*

In order to prove this theorem we need two lemmas.

Lemma 20.5. *Let P be a Sylow p -subgroup of a finite group G , and let $g \in G$ be an element whose order is a power of p . If $g^{-1}Pg = P$ then $g \in P$.*

Proof. The condition $g^{-1}Pg = P$ means that $g \in N(P)$, and so $\langle g \rangle \leq N(P)$. Since $P \trianglelefteq N(P)$, we can apply the Second Isomorphism Theorem, which gives

$$\frac{\langle g \rangle P}{P} \cong \frac{\langle g \rangle}{\langle g \rangle \cap P}.$$

Therefore

$$|\langle g \rangle P| = \frac{|\langle g \rangle| |P|}{|\langle g \rangle \cap P|},$$

and since both $|\langle g \rangle|$ and $|P|$ are powers of p , so is $|\langle g \rangle P|$. On the other hand, P has the maximal possible such an order, and therefore we conclude that $\langle g \rangle P = P$, which is equivalent to $g \in P$. ■

Lemma 20.6. *Let G be a group, and let $H, T \leq G$. The number of distinct conjugates of H of the form $t^{-1}Ht$ with $t \in T$ is $[T : T \cap N(H)]$.*

Proof. This is a generalisation of Theorem 18.4, and the proof is left as an exercise. ■

Proof of the second Sylow theorem. Let $|G| = p^n m$, where p is a prime and $\gcd(p, m) = 1$, and let P be an arbitrary Sylow p -subgroup of G .

To prove the first statement, we note that for $g \in G$ we have $g^{-1}Pg \cong P$ since conjugation by g induces an automorphism of G (Theorem 17.6). In particular, $|g^{-1}Pg| = |P| = p^n$, and hence $g^{-1}Pg$ is a Sylow p -subgroup.

For the converse statement, denote by $\mathcal{K} = \{P = P_1, P_2, \dots, P_k\}$ the set of all distinct conjugates of P . Assume that there exists a Sylow p -subgroup Q of G which is not in \mathcal{K} . Consider conjugation by elements of Q in \mathcal{K} . For any $P_i \in \mathcal{K}$, choose $q \in Q$ such that $q \notin P_i$; by Lemma 20.5 we then have $q^{-1}P_iq \neq P_i$. Therefore, each P_i has more than one conjugate by elements from Q . By Lemma 20.6, the number of conjugates of P_i by elements from Q is equal to $[Q : Q \cap N(P_i)]$. Since Q is a p -group, this number must be divisible by p . We conclude that conjugation by elements in Q partitions the set \mathcal{K} into the classes, each of which has a multiple of p elements. Therefore $k \equiv 0 \pmod{p}$.

Now consider the conjugation by elements from P . This time P is the only conjugate of itself, but the remaining elements of \mathcal{K} again split into groups, each having a multiple of p elements. This time we conclude that $k - 1 \equiv 0 \pmod{p}$, which is a contradiction with the conclusion of the last paragraph. Therefore, we conclude that \mathcal{K} contains all Sylow p -subgroups of G , and hence any two such subgroups are conjugate.

The third Sylow theorem discusses the number of Sylow p -subgroups.

Theorem 20.7 (The third Sylow theorem) *Let G be a finite group, and let p be a prime dividing the order of G . The number of Sylow p -subgroups of G divides $|G|$ and has the form $ps + 1$ for $s \geq 0$.*

Proof. Let P be a Sylow p -subgroup of G . By the second Sylow theorem, any other Sylow p -subgroup of G is a conjugate of P . By Theorem 18.4, the number of conjugates of P is $[G : N(P)]$, and this divides $|G|$ by Lagrange's theorem.

On the other hand, if $\mathcal{K} = \{P = P_1, P_2, \dots, P_k\}$ is the set of all Sylow p -subgroups of G , then we can consider the conjugation in \mathcal{K} by the elements of P . As in the proof of the second Sylow theorem, the only conjugate of P is P itself, and the rest of \mathcal{K} is partitioned into blocks, each block having a multiple of p elements. Therefore, k has the form $ps + 1$ for some $s \geq 0$.

■

Example 20.8. The symmetric group S_4 has order $24 = 2^3 \cdot 3$. Therefore, by the first Sylow theorem we conclude that S_4 contains Sylow 2-subgroups of order 8 and Sylow 3-subgroups of order 3. By the third Sylow theorem, the number of Sylow 3-subgroups divides 24 and is of the form $3k + 1$. Therefore, there are either one or four Sylow 3-subgroups. Now, each of eight three-cycles in S_4 generates a subgroup of order 3, and in this way we obtain 4 distinct subgroups of order 3 in S_4 . Therefore, S_4 contains 4 Sylow 3-subgroups.

Similarly, the number of Sylow 2-subgroups of S_4 is either 1 or 3, and one may check that there are actually three of them. (The group H from Example 6.7 is one of them.)

21. Applications of the Sylow Theorems

Sylow's Theorems are a powerful tool for investigating finite groups. We shall use them to classify the groups of order less than 16. First, however, we show how one can use Sylow's Theorems to prove non-existence of simple groups of certain orders. (Let us recall that a group is simple if it contains no proper normal subgroups.) The key observation here is the following:

Theorem 21.1. *Let G be a group and let P be a Sylow p -subgroup of G . Then P is normal in G if and only if P is a unique Sylow p -subgroup of G .*

Proof. P is normal $\Leftrightarrow P$ is closed under conjugation $\Leftrightarrow P$ is the only conjugate of itself.

On the other hand, by the Second Sylow's Theorem, any two Sylow p -subgroups of G are conjugate, and hence the theorem. ■

Example 21.2. There exists no simple group of order 200. Indeed, let G be a group of order $200 = 2^3 5^2$. By the Third Sylow's Theorem, the number of Sylow 5-subgroups of G divides 200 and has the form $5k + 1$. The divisors of 200 are 1, 5, 25, 2, 10, 50, 4, 20, 100, 8, 40, 200. The only number from the above list that has the form $5k + 1$ is 1. Therefore, G has a unique Sylow 5-subgroup, which is then normal in G by Theorem 21.1. This proves that G is not simple.

Example 21.3. There exists no simple group of order 12. For, assume to the contrary that G is a simple group of order $12 = 2^2 3$. By the Third Sylow's Theorem the number of Sylow 3-subgroups of G is either 1 or 4. Since G is simple, this number must be four because of Theorem 21.1. Each of these four subgroups has order 3, and is therefore isomorphic to \mathbb{Z}_3 . By Lagrange's Theorem, the intersection of any two of these subgroups must be trivial. Therefore, G has eight elements of order 3. Next, since G is not simple, it must contain at least two Sylow 2-subgroups H_1 and H_2 , each of them having order 4. By Lagrange's Theorem $H_1 \cap H_2$ has either one or two elements. Hence we conclude that G contains at least five elements of order a power of 2, which contradicts the fact that $|G| = 12$.

We can also prove the following nice characterisation of nilpotent groups.

Theorem 21.4. *A finite group is nilpotent \Leftrightarrow it is isomorphic to the direct product of p -groups.*

Proof. (Omitted in lectures)

(\Leftarrow) Every p -group is nilpotent by Theorem 19.6, and the direct product of nilpotent groups is again nilpotent by Theorem 16.9.

(\Rightarrow) Let G be a nilpotent group. Our first claim is that, for an arbitrary proper subgroup $H \leq G$, we have $N(H) \neq H$. Indeed, if we choose i so that $\gamma_i(G) \not\subseteq H$ but $\gamma_{i+1}(G) \subseteq H$, then we have

$$[\gamma_i(G), H] \subseteq [\gamma_i(G), G] = \gamma_{i+1}(G) \subseteq H.$$

Choose $x \in \gamma_i(G) \setminus H$. For every $h \in H$ we have $x^{-1}hxh^{-1} = [x, h] \in H$, and hence $x^{-1}hx \in Hh = H$. Therefore $x \in N(H) \setminus H$, as required.

Next we prove that every Sylow p -subgroup P of G is normal by showing that $N(P) = G$. Assume that $N(P) \neq G$. Then $N(P)$ is properly contained in $N(N(P))$ by the first claim. Let $x \in N(N(P)) \setminus N(P)$ be arbitrary. From $x \notin N(P)$ it follows that $x^{-1}Px$ is a Sylow p -subgroup distinct from P , while from $x \in N(N(P))$ and $P \subseteq N(P)$ it follows that $x^{-1}Px \subseteq N(P)$. This contradicts Lemma 20.5.

Assume that $|G| = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, and let P_i a Sylow p_i -subgroup of G ; by the previous paragraph we have $P_i \trianglelefteq G$. By Lagrange's Theorem we have $P_1 P_2 \dots P_n = G$ and $P_i \cap (P_1 \dots P_{i-1} P_{i+1} \dots P_n) = \{e\}$. Therefore, by Theorem 11.7 we have $G \cong P_1 \times \dots \times P_n$, a direct product of p -groups. ■

22. Groups of order pq

It is possible to classify all the groups of order pq , where p and q are distinct primes: there are at most two such groups, one of them is \mathbb{Z}_{pq} , and the other (if it exists) is a non-abelian group obtained by extending \mathbb{Z}_p by \mathbb{Z}_q in a way similar to direct products. Here, however, we shall not give this full classification, but shall rather restrict our attention to two special cases.

Theorem 22.1. *Let p and q be two distinct prime numbers, with $p > q$. If $p - 1$ is not divisible by q then \mathbb{Z}_{pq} is the only group of order pq .*

Proof. Let G be a group of order pq . By the Third Sylow Theorem the number of Sylow p -subgroups has the form $kp + 1$ and divides pq . Note that the divisors of pq are $1, p, q$ and pq . Since $p > q$ we must have $k = 0$, and so G has a unique Sylow p -subgroup H . By Theorem 21.1, H is normal in G ; also we have $H \cong \mathbb{Z}_p$ by Theorem 6.10.

Similarly, the number of Sylow q -subgroups is $kq + 1$ and divides pq . Clearly we cannot have $kq + 1 = q$ or $kq + 1 = pq$. However, we cannot have $kq + 1 = p$ either, because of the condition that q does not divide $p - 1$. So we are left with the only option of G having a unique Sylow q -subgroup K . As for H we now deduce that $K \trianglelefteq G$ and that $K \cong \mathbb{Z}_q$.

By Lagrange's Theorem, the order of $H \cap K$ must divide both $|H| = p$ and $|K| = q$, so that $H \cap K = \{e\}$. Also by Lagrange's Theorem, the order of HK is divisible by both p and q , and so is equal to pq , which means that $HK = G$. By Theorem 11.5 we now have $G \cong H \times K$, and hence $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ by Theorem 12.1. ■

Theorem 22.2. *Let $p > 2$ be a prime. The only groups of order $2p$ are the cyclic group \mathbb{Z}_{2p} and the dihedral group D_p .*

Proof. Let G be an arbitrary group of order $2p$. By the Third Sylow's Theorem, G has a unique Sylow p -subgroup N . This subgroup has order p , and is therefore cyclic. Let $a \in N$ be arbitrary, so that

$$N = \{e = a^0, a, a^2, \dots, a^{p-1}\}.$$

G also contains at least one element b of order 2. Clearly $b \notin N$, and since $[G : N] = 2$, it follows that N and Nb are the only cosets of N in G . Therefore

$$G = \{e = a^0, a, a^2, \dots, a^{p-1}, b, ab, a^2b, \dots, a^{p-1}b\}.$$

The number of Sylow 2-subgroups of G is either 2 or p . Let us consider these two possibilities separately.

Case 1: G has a unique Sylow 2-subgroup K . By Theorem 21.1 we have $K \trianglelefteq G$. By Lagrange's Theorem we must have $N \cap K = \{e\}$ and $NK = G$, so that $G \cong N \times K$ by Theorem 11.5. Since $N \cong \mathbb{Z}_p$ and $K \cong \mathbb{Z}_2$ we conclude that $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$ by Theorem 12.1.

Case 2: G has p Sylow 2-subgroups. This means that G has p elements of order 2. On the other hand none of the elements of N has order 2, so that all the elements from $G \setminus N$ have order 2. In particular, $b^2 = e$. But then from $a^i b a^i b = e$ we conclude that $b a^i = a^{p-i} b$, so that

$$(a^i b^j)(a^k b^l) = \begin{cases} a^{i+k} b^l & \text{if } j = 0 \\ a^{i-k+p} b^{l+1} & \text{if } j = 1. \end{cases}$$

This gives an explicit formula for the multiplication in G , and therefore G is uniquely determined. On the other hand D_p is a non-abelian group of order $2p$, and so $G \cong D_p$. ■

23. Groups of small orders

In this section we shall classify all the groups of order less than 16. In doing this we shall make use of the following general classification theorems proved so far:

- \mathbb{Z}_p is the only group of order p (Theorem 6.10);
- \mathbb{Z}_{p^2} and $\mathbb{Z}_p \oplus \mathbb{Z}_p$ are the only two groups of order p^2 (Theorem 19.4);
- \mathbb{Z}_{pq} is the only group of order pq if $p - 1$ is not divisible by q (Theorem 22.1);
- \mathbb{Z}_{2p} and D_p are the only two groups of order $2p$ (Theorem 22.2);

(p and q denote primes, with $p > q$).

Actually, the above results cover all the orders less than 16, apart from 8 and 12. We now deal with these two cases.

Theorem 23.1. *There are five non-isomorphic groups of order 8, namely \mathbb{Z}_8 , $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, Q_8 and D_4 .*

Proof. By the Fundamental Theorem for Finite Abelian Groups, every abelian group of order 8 is isomorphic to one of the groups \mathbb{Z}_8 , $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. So let us assume that G is a non-abelian group of order 8.

By Lagrange's Theorem, the possible orders for a non-identity element of G are 2, 4 and 8. However, G cannot contain an element of order 8, as G is not abelian, let alone cyclic. Also, a group in which every non-identity element has order 2 is abelian; see Tutorial 1, Question 2. We conclude that G contains an element a of order 4. The subgroup $N = \{e, a, a^2, a^3\}$ generated by a has index 2, and is therefore normal in G .

Let now $b \in G \setminus N$ be arbitrary. Then N and Nb are the cosets of N in G , and so

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Since $N \trianglelefteq G$, we must have $b^{-1}ab \in N$. We also know that $b^{-1}ab$ must have the same order as a does; see Tutorial 2, Question 1. Therefore, either $b^{-1}ab = a$ or $b^{-1}ab = a^3$. The former possibility leads to $ab = ba$, which is a contradiction with the assumption that G is non-abelian. We conclude that $b^{-1}ab = a^3$, i.e. $ba = a^3b$. Now we have

$$(a^i b^j)(a^k b^l) = \begin{cases} a^{i+k} b^l & \text{if } j = 0 \\ a^{i+3k} b & \text{if } j = 1, l = 0 \\ a^{i+3k} b^2 & \text{if } j = l = 1. \end{cases}$$

We see that the multiplication in G is uniquely determined once we know b^2 . Now, b^2 cannot be equal to $a^i b$, as this would imply $b = a^i$. Next, we cannot have $b^2 = a$, as this would imply $G = \langle b \rangle$. Finally, we cannot have $b^2 = a^3$, because it implies $b^6 = a^9 = a$, and so $G = \langle b \rangle$. Therefore b^2 is equal either to e or to a^2 , giving two possible multiplications on G . We conclude that there are at most two non-abelian groups of order 8.

On the other hand, the groups Q_8 and D_4 are non-abelian of order 8. Moreover, one may verify that they are not isomorphic just by looking at the orders of elements (see Tutorial 5, Question 5). Hence the theorem. ■

Now we turn our attention to groups of order 12. We already know that D_6 and A_4 are non-abelian of this order. The following example exhibits another group of order 12.

Example 23.2. Let T be the subgroup of S_{12} generated by the permutations $(1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9\ 10\ 11\ 12)$ and $(1\ 7\ 4\ 10)(2\ 12\ 5\ 9)(3\ 11\ 6\ 8)$. By using the standard method for calculating a group given by its generators we can see that

$$T = \{\text{id}, (1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9\ 10\ 11\ 12), (1\ 3\ 5)(2\ 4\ 6)(7\ 9\ 11)(8\ 10\ 12), \\ (1\ 4)(2\ 5)(3\ 6)(7\ 10)(8\ 11)(9\ 12), (1\ 5\ 3)(2\ 6\ 4)(7\ 11\ 9)(8\ 12\ 10), \\ (1\ 6\ 5\ 4\ 3\ 2)(7\ 12\ 11\ 10\ 9\ 8), (1\ 7\ 4\ 10)(2\ 12\ 5\ 9)(3\ 11\ 6\ 8), \\ (1\ 8\ 4\ 11)(2\ 7\ 5\ 10)(3\ 12\ 6\ 9), (1\ 9\ 4\ 12)(2\ 8\ 5\ 11)(3\ 7\ 6\ 10), \\ (1\ 10\ 4\ 7)(2\ 9\ 5\ 12)(3\ 8\ 6\ 11), (1\ 11\ 4\ 8)(2\ 10\ 5\ 7)(3\ 9\ 6\ 12), \\ (1\ 12\ 4\ 9)(2\ 11\ 5\ 8)(3\ 10\ 6\ 7)\}.$$

The orders of elements of T are 1, 2, 3, 3, 4, 4, 4, 4, 4, 4, 6, 6. Similarly, the orders of elements of D_6 and A_4 are 1, 2, 2, 2, 2, 2, 2, 2, 3, 3, 6, 6 and 1, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3 respectively. Therefore, we see that T is a group of order 12 which is not isomorphic to D_6 and A_4 .

Theorem 23.3. *The only groups of order 12 are \mathbb{Z}_{12} , $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$, D_6 , A_4 and T .*

Sketch of proof. By the Fundamental Theorem for Finite Abelian Groups, the only abelian groups of order 12 are $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$. So let G be a non-abelian group of order 12, let s_2 be the number of Sylow 2-subgroups of G , and let s_3 be the number of Sylow 3-subgroups of G . By the Third Sylow Theorem we have $s_2 = 1$ or $s_2 = 3$, and also $s_3 = 1$ or $s_3 = 4$.

If $s_2 = s_3 = 1$, then G has a unique Sylow 2-subgroup N and a unique Sylow 3-subgroup K . They are both normal in G , and a standard argument proves that $G \cong N \times K$. However, $|N| = 4$ and $|K| = 3$, and hence they are both abelian. But then so is G , which is a contradiction.

If $s_2 = 3$ and $s_3 = 4$, then G would have eight elements of order three, and a further six elements of order power of 2 (see Example 21.3). This contradicts the fact that $|G| = 12$.

If $s_2 = 1$ and $s_3 = 4$, then G has a unique Sylow 2-subgroup N of order 4. N is isomorphic either to \mathbb{Z}_4 or to K_4 . The former case, however, leads to a contradiction, and so $N \cong K_4$. By a standard argument one can now attempt to reconstruct the multiplication for G . One obtains two possibilities, but they turn out to define isomorphic groups. Therefore, in this case we obtain at most one group.

Finally, if $s_2 = 3$ and $s_3 = 1$, one obtains further two possible multiplications on G , thus giving a total of at most three non-abelian groups of order 12.

To complete the proof, one has to show that D_6 , A_4 and T are non-isomorphic, which can be done by calculating the orders of their elements.

■

We have completed our classification of groups of order less than 16. The results are summarised in Table 4.2. Let us mention that the number of groups of order 16 is 14, and the number of groups of order 32 is 51. There is no known formula giving the number of groups of order n .

order	groups	reference
1	$\langle e \rangle$	
2	\mathbb{Z}_2	Theorem 6.10
3	\mathbb{Z}_3	Theorem 6.10
4	$\mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$	Theorem 19.4
5	\mathbb{Z}_5	Theorem 6.10
6	$\mathbb{Z}_6, D_3 (= S_3)$	Theorem 22.2
7	\mathbb{Z}_7	Theorem 6.10
8	$\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	Theorem 23.1
9	$\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3$	Theorem 19.4
10	\mathbb{Z}_{10}, D_5	Theorem 22.2
11	\mathbb{Z}_{11}	Theorem 6.10
12	$\mathbb{Z}_{12}, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3, D_6, A_4, T$	Theorem 23.3
13	\mathbb{Z}_{13}	Theorem 6.10
14	\mathbb{Z}_{14}, D_7	Theorem 22.2
15	\mathbb{Z}_{15}	Theorem 22.1.

Table 4.2: groups of order ≤ 16